12 FAM 550
SECURITY INCIDENT PROGRAM

(TL:DS-81; 01-31-2002)

12 FAM 551 GENERAL

12 FAM 551.1 Purpose

(TL:DS-70; 10-01-2000)

The purpose of the Security Incident Program is to enhance the protection of classified information by identifying, evaluating, and assigning responsibility for breaches of security. The program implements, inter alia, Executive Order 12958, National Security Information, April 20, 1995.

12 FAM 551.2 Definitions

(TL:DS-70; 10-01-2000)

a. A "security incident" is a failure to safeguard classified materials in accordance with 12 FAM 500, 12 FAM 600, 12 FAH-6, 5 FAH-6, and other applicable requirements for the safeguarding of classified material. Security incidents may be judged as either security infractions or security violations (see 12 FAM 012, Legal Authorities).

b. A "security infraction" is a security incident that, in the judgment of DS/ISP/APB, does not result in actual or possible compromise of the information. For example, at the end of the workday, an employee leaves a security container unlocked and unattended, containing classified information, in an area which has been authorized for the storage of classified information (i.e., it meets the requirements of 12 FAM 530 or 12 FAH-6). No unauthorized entry was evidenced. This incident would be adjudicated as an infraction.

c. A "security violation" is a security incident that, in the judgment of DS/ISP/APB, results in actual or possible compromise of the information. For example, if an employee transmits a classified document over an unclassified facsimile machine, the incident would be adjudicated as a violation, as the possibility for electronic interception and transcription of the classified document is real.

d. A "three year moving window" defines the period of time in which the aggregate of valid (as adjudicated by DS/ISP/APB) security incidents will be counted toward security clearance review or referral to the Bureau of Human Resources (HR) for possible disciplinary action. The period will start on the date of the most recent incident and extend backwards for a period of 36 months, but not prior to October 1, 2000.

e. A "responsible security officer" is the regional security officer (RSO), post security officer (PSO), or Marine security guard (MSG) abroad; or a DS/DO security officer or DS/DO/SSD uniformed protection officer (UPO), DS/ISP security officer, or MSG domestically.

f. A "principal unit security officer" (PUSO) is a managerial level Department of State employee of a bureau that is designated, in writing, by the bureau executive director to administer the security program in that organization, and to maintain liaison with DS/ISP/APB. PUSOs may designate any number of unit security officers to assist in performing security duties.

g. A "unit security officer" (USO) is a Department of State employee designated by the PUSO to administer the security program in that sub-organization (see 12 FAM 563).

h. Weingarten Rights are rights afforded to an employee who is a member of a collective bargaining unit for which a union representative has exclusive representation rights. When the employee is to be personally interviewed and reasonably believes that the interview may result in disciplinary action against him and/or her, the investigating official shall give the employee the opportunity to be represented by the exclusive representative, if the employee so requests. This right is known as the Weingarten Right.

12 FAM 552 SECURITY INSPECTIONS

(TL:DS-70; 10-01-2000)

a. Cleared U.S. citizen security personnel designated by DS/IST/ISP, Marine security guards (MSGs), and/or U.S. citizen contract guards are responsible for conducting security inspections to ensure that classified information is properly protected.

b. Such security inspections shall be conducted of all offices, buildings, or other facilities that come under the jurisdiction of the Department of State worldwide on a routine basis, except those exempted under interagency agreements.

c. Employees are prohibited from locking desks, bookcases, and credenzas (see also 12 FAM 539, paragraph j).

12 FAM 553 REPORTING OF SECURITY INCIDENTS

12 FAM 553.1 Reporting Improperly Secured Classified Information

(TL:DS-81; 01-31-2002)

a. All security incidents will be reported to DS/ISP/APB. Employees must inform the appropriate security officer, orally or in writing, of any improper security practice that comes to the employee's attention in order that remedial action may be taken.

b. Upon discovery of improperly secured classified information or of other security incidents, the responsible security officer (e.g., regional security officer (RSO) or MSG abroad; DS/DO security officer, DS/DO/UPO, DS/ISP security officer, or MSG domestically) must complete Form OF-117, Notice of Security Incident (see 12 FAM Exhibit 553.1A). This form is unclassified and must be prepared as comprehensively and accurately as possible. At a constituent post, the post security officer (PSO) will perform these duties on behalf of the RSO and forward all copies of Form OF-117 and Form OF-118, Record of Incident (see 12 FAM Exhibit 553.1B), to the responsible RSO. At posts abroad, the RSO will submit a copy of both Forms OF-117 and OF-118 directly to DS/ISP/APB.

c. Abroad, the RSO or PSO at constituent posts will investigate the incident and complete Form OF-118, item 1, and forward it to the person(s) alleged to be responsible for the incident. The person(s) alleged to be responsible for the incident shall execute and sign Form OF-118, item 2, within three workdays. Item 2 of Form OF-118 allows the employee to provide any mitigating factors, such as lack of culpability, which he or she believes would be pertinent to the adjudication process. If the person(s) alleged to be responsible for the incident fail(s) or refuse(s) to sign the form within three workdays, the RSO will document this fact in the security officer comments on Form OF-118, item 3, and forward Form OF-118 to DS/ISP/APB. When the person(s) alleged to be responsible for the incident sign(s) item 2 of the form, the RSO will give the form to the employee's immediate supervisor for signature, and will then complete item 3 and send the form to DS/ISP/APB. In item 3, the RSO will report the results of his or her investigation in a brief summary, indicating

whether in his or her view there has been a valid security incident, and, if so, whether it should be considered a security infraction or violation.

d. Domestically, the UPO watch commander will submit to DS/ISP/APB, a copy of Form OF-117 when it is issued to an apparent offender. When DS/ISP/APB receives the record copy of Form OF-117, DS/ISP/APB will complete item 1 of Form OF-118 and pass it to the PUSO of the person(s) alleged to be responsible for the incident for the completion of item 2. The person(s) alleged to be responsible for the incident must sign item 2 within three workdays. If the person(s) alleged to be responsible for the incident fail(s) or refuse(s) to sign Form OF-118, the PUSO will indicate this omission in the security officer comments in item 3, and return the form to DS/ISP/APB. When the person(s) alleged to be responsible for the incident sign(s) item 2, the PUSO will give the form to the employee's immediate supervisor for signature. He or she should then complete item 3 and submit the form to DS/ISP/APB.

e. The RSO or PUSO will give a copy of the completed Form OF-118 to the person(s) alleged to be responsible for the incident.

f. Form OF-118 is unclassified and must include, at a minimum, the information required by the instructions printed on the reverse side. Any classified supplemental information must be provided under separate memorandum.

g. If, as part of the investigation of a security incident, an employee who is to be personally interviewed, is a member of a collective bargaining unit for which a union representative has exclusive representation rights, and the employee reasonably believes that the interview may result in disciplinary action against him and/or her, the investigating official shall give the employee the opportunity to be represented by the inclusive representative, if the employee so requests. This right is known as the Weingarten Right. When the employee invokes the Weingarten Right, the investigating official will allow a reasonable time for a union representative to attend the interview.

12 FAM 553.2 Examples of Security Incidents

(TL:DS-77; 07-26-2001)

a. Listed in this section are examples of security incidents, in accordance with 12 FAM 500, that affect the protection of classified information. The examples are illustrative and intended to indicate the wide range of possible security incidents in this area. Information systems security incidents are discussed separately in 12 FAM 553.4.

b. Examples of security incidents are as follows:

(1) Failing to properly escort uncleared visitors or allowing improper access to Department of State controlled facilities (see 12 FAM 531);

(2) Taking classified material out of the building without proper double-wrap protection (see 12 FAM 539.4-1, paragraph a);

(3) Crossing international borders with classified material without courier authorization (see 12 FAM 536.9-1, paragraph a);

(4) Failing to secure containers with classified material (see 12 FAM 539.1, paragraph e);

(5) Storing classified materials in desk drawers or other improper containers (see 12 FAM 539.1, paragraph h);

(6) Failing to secure classified computer hard drives (see 12 FAM 539.1I);

(7) Reading classified material in any public area (see 12 FAM 536.9, paragraph e);

(8) Transmitting classified material on unclassified facsimile machines (see 12 FAM 536.9-2 and 536.9-3);

(9) Losing control of classified material by leaving it in non-secure areas, such as hotel rooms, taxis, or restaurants (see 12 FAM 533.1 and 534.1);

(10) Placing classified information on unclassified computers (see 12 FAM 531, paragraph c); and

(11) Discussing classified information on unsecure telephones (see 12 FAM 536.8, paragraph c).

(12) Failure to check supplemental entry verification systems (SEVs) daily (see 12 FAH-6 H-311.11 d, H-312.11 d, H-313.11 d, and H-314.11 d).

12 FAM 553.3 Information System Security Incidents

(TL:DS-70; 10-01-2000)

Listed in this subsection are examples of security incidents, in accordance with 12 FAM 600, that affect the protection of classified information with respect to information systems. The following examples are illustrative and intended to indicate the wide range of possible security incidents in this area:

(1) Failure to remove and properly secure media, normally controlled by users such as, classified printer ribbons and data storage media, e.g., disk pack, hard drives, floppy disk, tape, ZIP disk, CD ROM, etc (see 12 FAM 638.1-4, paragraph b);

(2) Failure to prevent viewing by uncleared persons of a classified screen and/or printer output (see 12 FAM 638.3-2);

(3) Failure to label classified media (storage media, printer ,and typewriter ribbons) and hardware with the correct classification (see 12 FAM 528.2, paragraph a);

(4) Failure to log off a classified terminal and leaving it unattended (see 12 FAM 638.1-3, paragraph b);

(5) Improper storage of passwords to classified automated information systems (see 12 FAM 632.1-4, paragraph e.);

(6) Unauthorized connectivity between classified and unclassified hardware (e.g., modems, central processing units, printers, and switch boxes) (see 12 FAM 626.1-4); and

(7) Introducing classified media without proper authorization into an unclassified system (see 12 FAM 625.2-1, paragraph e).

12 FAM 553.4 Incidents Involving Administratively Controlled ("Sensitive But Unclassified") (SBU) Material

(TL:DS-70; 10-01-2000)

Security incident procedures described in this section do not pertain to Sensitive But Unclassified (SBU) material. Form OF-117 will not be issued for incidents involving SBU materials. (See 12 FAM 540 regarding the requirements for SBU materials.)

12 FAM 554 SPECIAL CATEGORY SECURITY

VIOLATIONS

12 FAM 554.1 Mishandling of Special Categories of Classified Information

(TL:DS-70; 10-01-2000)

Any security incident involving the mishandling of Top Secret, Special Access Program, and Special Compartmented Information (SCI) material will be deemed to be a security violation rather than an infraction, even when occurring in a controlled access area (CAA) abroad or within the equivalent of a CAA domestically.

12 FAM 554.2 Communications Security Violations

(TL:DS-73; 03-15-2001)

a. The following COMSEC security incidents, when adjudicated as valid, will be deemed to be security violations:

(1) Transmitting classified information over a communication channel that is unauthorized for the level of information being transmitted (see 5 FAH-6 H-553);

(2) Filing a false destruction report (see 5 FAH-6 H-553, III g);

(3) Leaving cryptographic key (i.e., the physical paper tape or electronic keying device), cryptographic material or COMSEC manuals unsecured (see 5 FAH-6 H-553, III b and d);

(4) Utilizing a superseded cryptographic key material on active classified networks (see 5 FAH-6 H-535.1 (2));

(5) Not reporting an inadvertently opened sealed package of, or extracted cryptographic keying material (see 5 FAH-6 H-527.6-3 (2));

(6) Failure to submit a cryptographic material inventory (see 5 FAH-6 H-123.2 d(1)); and

(7) Unauthorized installation of STU-III or other similar Type 1 encryption device outside of a CAA which is keyed to higher than an unclassified/privacy mode (see 5 FAH-6 H-565).

(8) Failure to perform a “change of custodian” inventory prior to the

scheduled departure of a primary COMSEC custodian domestically or abroad. (See 5 FAH-6 H-313.2.)

b. Abroad, COMSEC custodians or inspectors shall report any of the above such violations immediately by telegram to DS/ISP/APB with a copy to the RSO and the Office of Technical Operations (IRM/OPS/ITI/SI/CSB). Domestically, such violations must be reported by the COMSEC custodian immediately by telephone or FAX to DS/ISP/APB and IRM/OPS/ITI/SI/CSB. If the incident involves another agency, an information report must also be provided to that organization's Office of Security.

12 FAM 555 SECURITY INCIDENTS INVOLVING NONDEPARTMENT OF STATE EMPLOYEES AND CONTRACTORS

(TL:DS-77; 07-26-2001)

a. Security incidents involving employees of other Federal agencies or organizations and/or their contractors are reported in the same manner as described in 12 FAM 553. Thus, RSOs abroad will report all such incidents, together with Form OF-117 and Form OF-118, to DS/ISP/APB. DS/ISP/APB will coordinate any further investigation necessary to complete the report of findings. DS/ISP/APB will then forward the report of findings to the appropriate parent agency for adjudication and disposition.

b. Security incidents involving Department of State contractors are reported in the same manner as described in 12 FAM 553 above, except that DS/ISP/APB will forward Forms OF-117 and OF-118 to the employer with a copy of each to the DS Information Security Program's Industrial Security Branch (DS/ISP/INB).

12 FAM 556 EVALUATION OF SECURITY INCIDENTS

(TL:DS-70; 10-01-2000)

a. DS/ISP/APB will perform the final adjudication of all security incidents and initiate any further action, as required.

b. A basic premise for any adjudication is that individuals will be held

responsible for their actions. However, in certain incidents, supervisors may be held responsible for failure to provide effective organizational security procedures. This might occur, for example, when abnormal conditions cause an interruption of routine security procedures and remedial controls are not implemented, or when the incident relates to controls that are not normally the sole responsibilities of any individual.

c. DS/ISP/APB will notify the employee of the final outcome.

12 FAM 557 ADMINISTRATIVE ACTIONS

12 FAM 557.1 Record Keeping and Administrative Action Framework

(TL:DS-70; 10-01-2000)

a. DS/ISP/APB will maintain files on all personnel who have incurred security incidents. Upon employee termination, the records will be retired. Information from these files will be made available to the Director General of the Foreign Service or HR, as may be needed for future nominations or other personnel decisions, and will be included in full field investigation reports on candidates for Presidential appointment.

b. Disciplinary and security clearance actions for security incidents will be handled on a case by case basis, but in principle will become more serious following additional incidents.

c. An employee's adverse security incident history may result in the curtailment of a current assignment or denial of future assignments.

12 FAM 557.2 Referral for Disciplinary Actions and Security Clearance Review Related to Security Infractions

(TL:DS-70; 10-01-2000)

After affirmative adjudication by DS/ISP/APB of security infractions within a moving three year (36 month) window, at a minimum, DS will take the following actions:

(1) First infraction—The DS/ISP Division Chief will send a letter of warning to the employee requiring a signed reply from the employee acknowledging that the employee understands the

policies and ramifications of future security incidents. The RSO or PSO abroad, or USO domestically, will provide the employee with a security briefing.

(2) Second infraction—The DS/CIS Deputy Assistant Secretary will send a letter to the employee that includes a statement concerning DS and the actions the Bureau of HR will take in the event of future security incidents. This requires a signed reply from the employee indicating that the employee understands the policies and ramifications of future security incidents. The RSO or PSO abroad, or USO domestically, will provide the employee with an additional security briefing.

(3) Third and subsequent infractions within the 36 month window—DS/ISP/APB will refer the matter to the Bureau of HR for appropriate disciplinary action. DS/ISP/APB will also refer the matter to the Director of the DS Office for Investigations and Counterintelligence (DS/DSS/ICI) for appropriate action relating to the employee's security clearance.

12 FAM 557.3 Referral for Disciplinary Actions and Security Clearance Review Related to Security Violations

(TL:DS-70; 10-01-2000)

After affirmative adjudication by DS/ISP/APB that a security violation has occurred, DS/ISP/APB will refer the incident, along with a summary of mitigating or aggravating factors and other security incidents within the moving three year window, to DS/DSS/ICI and/or the Bureau of HR. DS/DSS/ICI and/or HR will take or initiate one or more of the actions listed below against the violator:

(1) DS will issue a letter of warning, review the security clearance of the violator, suspend or revoke the violator's security clearance; or

(2) HR will issue a letter of admonishment or a letter of reprimand, suspend the violator without pay, or terminate the violator's employment.

12 FAM 557.4 Appeals

(TL:DS-70; 10-01-2000)

a. Without prejudice to any other procedures, an employee wishing to

appeal the validity or categorization of a security incident may do so by submitting the appeal in writing to DS/ISP/APB. This must be done immediately after receiving notice that DS/ISP/APB has adjudicated the incident.

NOTE: An employee statement on Form OF-118 does not initiate an appeal procedure.

b. DS/ISP/APB will forward the appeal along with any other pertinent data to the Director, DS/CIS/IST, for a final appeal decision.

12 FAM 558 CRIMINAL LAWS

(TL:DS-70; 10-01-2000)

Incidents involving intentional or grossly negligent release or mishandling of classified information may be subject to criminal penalties. An illustrative list of criminal statutes establishing penalties of fine and imprisonment for the release of classified information is set forth in 12 FAM 558 Exhibit 558.

12 FAM 559 UNASSIGNED

12 FAM 553 EXHIBIT 553.1A FORM OF-117, NOTICE OF SECURITY INCIDENT

(TL:DS-70; 10-01-2000)

NOTICE OF SECURITY INCIDENT	Building or Post		Incident Number	
	Room		Office Occupying Room	
Suspected Person	Telephone #	Classification	Date (mm-dd-yyyy)	Time

Nature of Incident

Overseas: CAA ☐ Yes ☐ No Domestic: Area Locked ☐ Yes ☐ No Area Alarmed ☐ Yes ☐ No

Comments (Describe exactly where material was found.)

Print Name of Reporting Official	Signature of Reporting Official

OPTIONAL FORM 117
5-95
STATE-USAID

PLEASE ADVISE YOUR RSO/PSO OR USO OF THIS NOTICE

12 FAM 553 EXHIBIT 553.1B FORM OF-118, RECORD OF INCIDENT REPORT

(TL:DS-70; 10-01-2000)

INCIDENTS	*CODE*
UNSECURED SAFE OR BARLOCK *(Specify)*	**USF**
UNSECURED DISKS/DISKETTES	**UDD**
UNSECURED BURN BAG	**UBG**
UNSECURED DOCUMENTS	**UDC**
UNSECURED SAFE COMBINATIONS	**USC**
CLASSIFIED MATERIAL IN WASTEBASKET	**WAB**
UNSECURED VAULT DOOR	**UVD**
POUCH VIOLATION	**POD**
TRANSMISSION INCIDENT	**TRS**
MISCELLANEOUS	**MIS**

INSTRUCTIONS

Part 1.--Upon receiving a Report of Incident, the Post/Unit/Regional Security Officer shall immediately conduct a thorough investigation of the circumstances to determine who was responsible for the incident and to ascertain the possibility or extent of compromise. In Part 1 of this form, the security officer shall give a brief summary of the results of the investigation, which must include but *need not be limited to* the following details:

a. Name of persons suspected of committing incident.
b. Parent agency of person(s) suspected of committing incident *(do not use initials).*
c. Highest classification involved.
d. Investigating officer's estimate of the possibility of compromise (if compromise was possible, the investigating officer must also follow the procedures required by 12 FAM 553.2).
e. Identity of unauthorized person who could possibly have had access to unsecured material.
f. Time during which material was without required protection.
g. Description of action taken to prevent recurrences.

Part 2.--The employee suspected of the incident may make any comment he or she wishes in Part 2, including any mitigating circumstances. The employee shall then sign in the space provided and obtain the signature of his or her immediate supervisor. The employee must return the completed form to the Post/Unit/Regional Security Officer *within three working days.*

DISSEMINATION OF COMPLETED RECORD

Domestically, the Unit Security Officers shall forward the original of the completed Record of Incident to DS/ISP/APB.

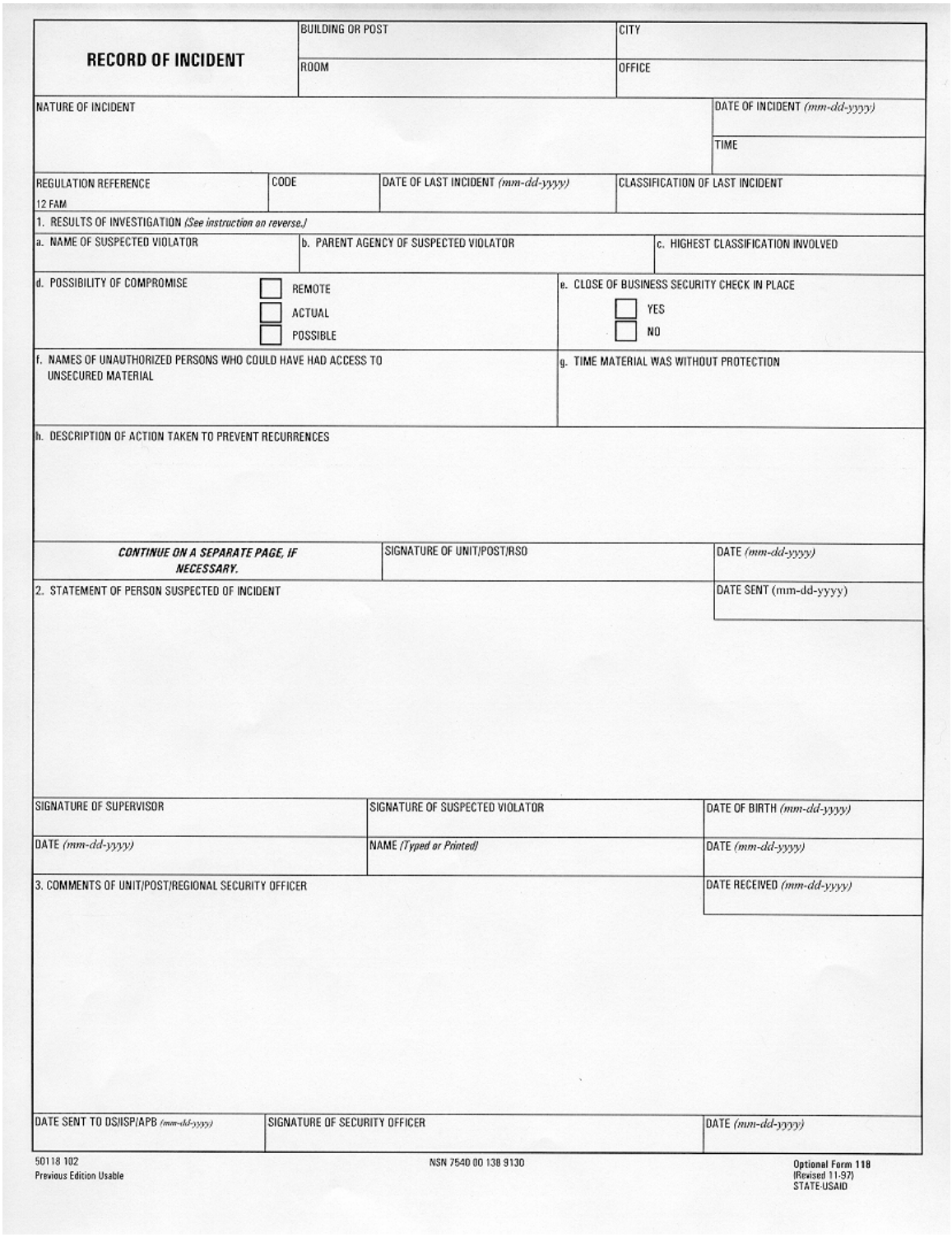
Violations Overseas: The Post Security Officer shall forward the original of the completed form to the Regional Security Officer. The Regional Security Officer, in turn, shall include his or her comments in Part 3. The Regional Security Officer will then forward the original to the Department, DS/ISP/APB, return one copy to the post for inclusion in the post incident file, retain one copy for his or her own files, and forward one copy to the violator.

Infractions Overseas: The Post/Regional Security Officer shall maintain a file of Security Infractions until an individual receives his or her FOURTH infraction or an aggreate of four incidents within an 18-month period. While an individual receives their fourth incident, all OF-118's will be forwarded to the Department, DS/ISP/APB for processing.

50118 102
Previous Edition Usable

NSN 7540 00 138 9130

Optional Form 118
(Revised 11-97
STATE-AID



RECORD OF INCIDENT

	BUILDING OR POST	CITY
	ROOM	OFFICE

NATURE OF INCIDENT	DATE OF INCIDENT *(mm-dd-yyyy)*
	TIME

REGULATION REFERENCE 12 FAM	CODE	DATE OF LAST INCIDENT *(mm-dd-yyyy)*	CLASSIFICATION OF LAST INCIDENT

1. RESULTS OF INVESTIGATION *(See instruction on reverse.)*

a. NAME OF SUSPECTED VIOLATOR	b. PARENT AGENCY OF SUSPECTED VIOLATOR	c. HIGHEST CLASSIFICATION INVOLVED

d. POSSIBILITY OF COMPROMISE ☐ REMOTE ☐ ACTUAL ☐ POSSIBLE	e. CLOSE OF BUSINESS SECURITY CHECK IN PLACE ☐ YES ☐ NO
f. NAMES OF UNAUTHORIZED PERSONS WHO COULD HAVE HAD ACCESS TO UNSECURED MATERIAL	g. TIME MATERIAL WAS WITHOUT PROTECTION

h. DESCRIPTION OF ACTION TAKEN TO PREVENT RECURRENCES

CONTINUE ON A SEPARATE PAGE, IF NECESSARY.	SIGNATURE OF UNIT/POST/RSO	DATE *(mm-dd-yyyy)*

2. STATEMENT OF PERSON SUSPECTED OF INCIDENT	DATE SENT (mm-dd-yyyy)

SIGNATURE OF SUPERVISOR	SIGNATURE OF SUSPECTED VIOLATOR	DATE OF BIRTH *(mm-dd-yyyy)*
DATE *(mm-dd-yyyy)*	NAME *(Typed or Printed)*	DATE *(mm-dd-yyyy)*

3. COMMENTS OF UNIT/POST/REGIONAL SECURITY OFFICER	DATE RECEIVED *(mm-dd-yyyy)*

DATE SENT TO DS/ISP/APB *(mm-dd-yyyy)*	SIGNATURE OF SECURITY OFFICER	DATE *(mm-dd-yyyy)*

50118 102
Previous Edition Usable

NSN 7540 00 138 9130

Optional Form 118
(Revised 11-97)
STATE-USAID

12 FAM 558 EXHIBIT 558
CRIMINAL LAWS

(TL:DS-61; 10-01-1999)

Penalties of fine and imprisonment are established by statute for the unauthorized disclosure, dissemination, communication, furnishing, transmission, or other unlawful release of certain classified information, and for making false or fraudulent statements to an agency of the Government. Employees are admonished to read the following provisions of such laws:

18 U.S.C.

Section 641. Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts to his use, or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—

Shall be fined not more than $10,000 or imprisoned not more than ten years or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

Section 793. Gathering, transmitting or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction

by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative. blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or cause(s) to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted to the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined not more than $10, 000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy, shall be subject to the punishment provided for the offense which is the object of such conspiracy.

Section 794. Gathering or delivering defense information to aid foreign government

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof,

either directly or indirectly, any document, writing, code book, signal book, sketch, note, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any if naval or military operations or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c)If two or more persons conspire to violate this section, and one or more of such person is do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

Section 798. Disclosure of Classified Information

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or uses in any manner prejudicial to the safety or interest of the United States for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the process of communication intelligence from the

communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in their meanings, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

Section 952. Diplomatic codes and correspondence

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official

diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

50 U.S.C.

Subchapter IV—Protection Of Certain National Security Information

Section 421. Protection of Identities of Certain United States Undercover Intelligence Officers, Agents, Informants, and Sources

(a) Disclosure of information by persons having or having had access to classified information that identified covert agent

Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $50,000 or imprisoned not more than ten years, or both.

(b) Disclosure of information by persons who learn identity of covert agent as a result of having access to classified information

Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $25,000 or imprisoned not more than five years, or both.

(c) Disclosure of information by persons in course of pattern of activities intended to identity and expose covert agents

Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies and individual as a covert agent to any individual not authorized to receive

classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined not more than $15,000 or imprisoned not more than three years, or both.

Section 422. Defenses and Exceptions

(a) Disclosure by United States of identity of covert agent

It is a defense to a prosecution under section 421 of this title that before the commission of the offense with which the defendant is charged, the United States had publicly acknowledged or revealed the intelligence relationship to the United States of the individual the disclosure of whose intelligence relationship to the United States is the basis for the prosecution.

(b) Conspiracy, misprision of felony, aiding and abetting, etc.

(1) Subject to paragraph (2), no person other than a person committing an offense under section 421 of this title shall be subject to prosecution under such section by virtue of section 2 or 4 of title 18, United States Code, or shall be subject to prosecution for conspiracy to commit an offense under such section.

(2) Paragraph (1) shall not apply (A) in the case of a person who acted in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, or (B) in the case of a person who has authorized access to classified information.

(c) Disclosure to select Congressional committees on intelligence

It shall not be an offense under section 421 of this title to transmit information described in such section directly to the Select Committee on Intelligence of the House of Representatives.

(d) Disclosure by agent of own identity

It shall not be an offense under section 421 of this title for an individual to disclose information that solely identifies himself as a covert agent.

Section 423. Report

(a) Annual report by President to Congress on measures to protect

identities of covert agents

The President, after receiving information from the Director of Central Intelligence, shall submit to the Select Committee on Intelligence of the House of Representatives an annual report on measures to protect the identities of covert agents, and on any other matter relevant to the protection of the identities of covert agents.

(b) Exemption from disclosure; date of initial submission

The report described in subsection (a) of this section shall be exempt from any requirement for publication or disclosure. The first such report shall be submitted no later than February 1, 1983.

Section 424. Extraterritorial Jurisdiction

There is jurisdiction over an offense under section 421 of this title committed outside the United States if the individual committing the offense is a citizen of the United States or an alien lawfully admitted to the United States for permanent residence (as defined in section 1101(a)(20) of title 8).

Section 425. Providing Information to Congress

Nothing in this title may be construed as authority to withhold information from

Section 426. Definitions

For the purposes of this subchapter:

(1) The term “classified information” means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a stature or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(2) The term “authorized”, when used with respect to classified information, means having authority, right, or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representative or resolution of the Senate which assigns responsibility within the respective House of Congress for the oversight of intelligence activities.

(3) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(4) The term "covert agent" means—

(A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency—

(i) whose identity as such an officer, employee, or member is classified information, and

(ii) who is serving outside the United States or has within the last five years served outside the United States; or

(B) a United States citizen whose intelligence relationship to the United States is classified information, and—

(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(5) The term "intelligence agency" means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.

(6) The term "informant" means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms "officer" and "employee" have the meanings given such terms by section [sic] 2104 and 2105, respectively, of title 5, United States Code.

(8) The term "Armed Forces" means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

(9) The term "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(10) The term "pattern of activities" requires a series of acts with a common purpose or objective.

Section 783. Offenses

(b) Communication of classified information by Government officer or employee

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or any officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee in employed, to make such disclosure of such information.